Como categorizar un Sistema en el ENS

Esta es una de las tareas que más "pánico" le produce a cualquier organismo de la Administración y es en realidad uno de los primeros pasos a la hora de implantar el ENS, pues de esta categorización dependerán muchas de las medidas a implantar tanto del marco operacional como de las medidas de protección.

Según el ***Anexo I. RD 3/2010***

1. *Fundamentos para la determinación de la categoría de un sistema.*
   La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para:
   a. *Alcanzar sus objetivos.*
   b. *Proteger los activos a su cargo.*
   c. *Cumplir sus obligaciones diarias de servicio.*
   d. *Respetar la legalidad vigente.*
   e. *Respetar los derechos de las personas.*

Lo que tenemos que hacer es valorar el ***impacto*** que tendría un incidente que afecte a la seguridad de la información y los sistemas. Para determinar ese ***impacto*** hay que tener en cuenta las dimensiones de la seguridad: Disponibilidad [D], Integridad [I], Confidencialidad [C], Autenticidad [A], Trazabilidad [T], en adelante [DICAT]

El ***impacto*** que tendría un incidente que pudiese ocurrir sobre cada información o cada servicio pueden afectar a una o más de sus dimensiones de seguridad y cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

Un grupo de Información y/o Servicio formarán un sistema de información a categorizar, por tanto podemos confeccionar una tabla como la que sigue en donde para cada información y/o servicio de los que formarían nuestro sistema, establecemos como sería el nivel del ***impacto*** (*Bajo, Medio o Alto*) que un incidente produciría en cada una de las dimensiones de seguridad a tener en cuenta.

	DIMENSIONES				
SISTEMA	Disponibilidad [D]	Integridad [I]	Confidencialidad [C]	Autenticidad [A]	Trazabilidad [T]
Información A	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto
Información B	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto
…	…	…	…	…	…
Servicio X	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto
Servicio Y	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto
…	…	…	…	…	…

Tabla 1

Ahora sólo debemos tener en cuenta lo que significa cada dimensión y para cada una, que significan los niveles de impacto Bajo, Medio y Alto.

a) Nivel BAJO.
Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio limitado:
    1. La reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.
    2. Que los activos de la organización sufrieran un daño menor.
    3. El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
    4. Causar un perjuicio menor a algún individuo, que aún siendo molesto pueda ser fácilmente reparable.
    5. Otros de naturaleza análoga.

b) Nivel MEDIO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio grave:
    1. La reducción significativa la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.
    2. Que los activos de la organización sufrieran un daño significativo.
    3. El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
    4. Causar un perjuicio significativo a algún individuo, de difícil reparación.
    5. Otros de naturaleza análoga.

c) Nivel ALTO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio muy grave:
    1. La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.
    2. Que los activos de la organización sufrieran un daño muy grave, e incluso irreparable.
    3. El incumplimiento grave de alguna ley o regulación.
    4. Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
    5. Otros de naturaleza análoga

Cuando un sistema maneje diferentes informaciones y preste diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

a) Un sistema de información será **de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.**
b) Un sistema de información será **de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.**
c) Un sistema de información será **de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.**

Para ello podemos usar la ***GUÍA DE SEGURIDAD (CCN-STIC-803). ESQUEMA NACIONAL DE SEGURIDAD. VALORACIÓN DE LOS SISTEMAS*.**

…/…

6. Con frecuencia, el valor del sistema en materia de seguridad se concentra en unos pocos activos que son la esencia y razón de ser del sistema, y en unas pocas dimensiones. ***Es conveniente centrarse en aquellos activos y en aquellas dimensiones en las que el impacto de un incidente sea mayor, obviando aquellas combinaciones en las que el impacto sea despreciable o irrelevante.***

7. ***Conviene comenzar por los activos de tipo información, valorando en este orden: confidencialidad, integridad, autenticidad, trazabilidad y, si fuera relevante, disponibilidad. Es frecuente que la disponibilidad no sea un atributo relevante de la información y quede sin adscribir a ningún nivel.***

8. ***Conviene seguir con los activos de tipo servicio, valorando en este orden: disponibilidad, autenticidad y trazabilidad. Los requisitos en materia de confidencialidad e integridad suelen venir impuestos por la información que maneja el servicio, heredándose los establecidos en el párrafo anterior.***

9. El sistema queda valorado por los valores máximos de la información que maneja y los servicios que presta.

…/…

Extraído de la GUÍA DE SEGURIDAD (CCN-STIC-803).

Con lo cual, ya tenemos las primeras acciones a realizar para valorar el sistema, y con estos puntos de la guía establecemos un orden.

Nota personal:

> *Solo hay una cosa son la que discrepo y hablo por experiencia propia "…****Es frecuente que la disponibilidad no sea un atributo relevante de la información y quede sin adscribir a ningún nivel."*** *En el caso del organismo donde trabajo, existe una información en base a la cual se toman decisiones críticas y su disponibilidad es más que alta, altísima.*

Ya sabemos que:

- Es conveniente centrarse en aquellos activos y en aquellas dimensiones en las que el impacto de un incidente sea mayor, obviando aquellas combinaciones en las que el impacto sea despreciable o irrelevante.
- El orden:
  - Primero los activos de tipo información, valorando los en este orden: confidencialidad, integridad, autenticidad, trazabilidad y, si fuera relevante, disponibilidad.
  - Después los activos de tipo servicio, valorando los en este orden: disponibilidad, autenticidad y trazabilidad. Los requisitos en materia de confidencialidad e integridad suelen venir impuestos por la información que maneja el servicio.

Lo que nos lleva a la siguiente pregunta:

QUIEN DEBE VALORAR… Información y/o Servicios

…/…

10. Si el organismo ha creado un Comité TIC (Comité Técnico) y un Comité STIC (Comité de Seguridad de la Información), una de las funciones del comité TIC puede ser la determinación de los tipos de información que se van a manejar y una clasificación de los servicios que se van a prestar. Definidos los tipos de información y de servicios, una tarea del Comité STIC puede ser el establecimiento de los niveles de seguridad recomendados para cada uno de los tipos de información y servicios. Estas definiciones deben ser aprobadas dentro del juego de normativa que rige las actuaciones del organismo.

11. Los niveles así establecidos podrán ser posteriormente ajustados por los responsables correspondientes. Idealmente, todas las valoraciones vendrán establecidas por la normativa.

12. ***La responsabilidad de la valoración de la información y de los servicios es exclusivamente del responsable correspondiente. La valoración puede ser propuesta por el Responsable del Sistema o por el Responsable de Seguridad y aprobada por el responsable de la información o del servicio correspondiente si éste la considera adecuada.***

…/…

Extraído de la GUÍA DE SEGURIDAD (CCN-STIC-803).

Ya que "**La valoración puede ser propuesta por el Responsable del Sistema o por el Responsable de Seguridad",** un buen método es acudir a los responsables de la Información y/o Servicio, con una "pre-propuesta".

Dado que aquello que hay que valorar son Información y Servicios podemos dividir la tarea en dos: Valorar la información y valorar los servicios.

Para VALORAR LA INFORMACIÓN

…/…

18. No se valorarán directamente datos auxiliares que no son objeto directo del proceso administrativo y sólo aparecen como instrumentales para la prestación de los servicios. Por ejemplo, servicios de directorio, claves de acceso, etc.

19. Para cada elemento de información, se debe determinar:

- *Su nombre, que la identifica unívocamente*
- *Su responsable, que establece sus requisitos de seguridad*
- *Otras características que se consideren relevantes a efectos operacionales, de asociación de vulnerabilidades, de estimación de riesgos o de auditoría*

22. ***La información suele imponer requisitos relevantes en las dimensiones de confidencialidad, integridad, autenticidad y trazabilidad.*** *No suelen haber requisitos relevantes en la dimensión de disponibilidad.*

23. El nivel de seguridad requerido en el aspecto de ***confidencialidad se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.***

24. El nivel de seguridad requerido en el aspecto de ***integridad se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.***

25. El nivel de seguridad requerido en el aspecto de ***autenticidad se establecerá en función de las consecuencias que tendría el hecho de que la información no fuera auténtica.***

26. El nivel de seguridad requerido en el aspecto de ***trazabilidad se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido a o modificado una cierta información.***

27. El nivel de seguridad requerido en el aspecto de ***disponibilidad se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera acceder a la información cuando la necesita.***

28. Cuando un aspecto no requiere medidas de seguridad, en el apartado de valoración se indicará SIN VALORAR.

…/…

Extraído de la GUÍA DE SEGURIDAD (CCN-STIC-803).

Con lo cual hemos quitado de golpe aquello que tanto nos preocupa ***"Por ejemplo, servicios de directorio, claves de acceso, etc."*** Para centrarnos sólo en lo que a nivel de categorización importa.

Seguramente, se os plantee la duda ¿qué hacer si los datos contienen información de carácter personal?

La propia Guía 803 establece que para los DATOS DE CARÁCTER PERSONAL, muchas de las medidas que tomemos, pueden ser compartidas.

…/…

115. Los datos de carácter personal tienen su propia legislación:

- *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. Nº 298, de 14 de diciembre de 1999)*
- *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*

116. De acuerdo dicha regulación, los datos de carácter personal requieren una serie de medidas de seguridad de un cierto nivel determinado por su naturaleza y la finalidad con la que se manejan.

*117**. Muchas medidas de seguridad vienen requeridas tanto por el Esquema Nacional de Seguridad como por el Reglamento de Protección de Datos de Carácter Personal, por lo que su implantación puede ser unificada, sin perjuicio de que en los procesos de auditoría se verifique su idoneidad para proteger tanto los datos de carácter personal como los servicios prestados a los ciudadanos.***

*118. **Es función del responsable de seguridad determinar el conjunto de medidas requerido, uniendo los que se requieren por una y otra norma, e imponiendo la exigencia superior.***

119. La existencia de datos de carácter personal requiere la realización de un documento de seguridad y la designación de una serie de responsables. Parece natural que estos requisitos se contemplen en la Política de Seguridad requerida por el Esquema Nacional de Seguridad.

…/…

Extraído de la GUÍA DE SEGURIDAD (CCN-STIC-803).

Pero podríamos hacerlo por separado si conviene a nuestros intereses, ya que aplicar medidas en cuanto a la protección de datos de carácter personal de nivel ALTO, podría llevarnos si lo hacemos en conjunto a categorizar el sistema como de nivel ALTO, y entonces (aunque el perjuicio estaría en la sobreprotección del sistema), eso nos llevaría a implementar medidas tanto del marco operacional como de las medidas de protección de nivel alto, y seguramente eso implicaría un sobre coste.

Busque la respuesta en el documento de preguntas frecuentes sobre el ENS que ha editado el CCN y efectivamente, puede hacerse por separado.

…/…

3.1. ¿Se pueden entender equivalentes los niveles LOPD con los niveles ENS?

Las denominaciones BÁSICO/MEDIO/ALTO, que utilizan tanto el ENS como el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (Real Decreto 1720/2007, de 21 de diciembre, por el que se

aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal), no poseen la misma semántica. Es decir: no son intercambiables ni significan lo mismo.

Así, mientras que para el RD 1720/2007 los niveles de seguridad se determinan por la pertenencia del dato a un nivel concreto, para el ENS la categoría del sistema se sustenta en el impacto que un incidente de seguridad podría tener en relación con la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio y el respeto a la legalidad y a los derechos de los ciudadanos (y en sus dimensiones: integridad, confidencialidad, trazabilidad, disponibilidad y autenticidad). Por tanto, puesto que su determinación obedece a procedimientos distintos, cada sistema/servicio/tratamiento debe cualificarse independientemente:

Para su conformidad con la normativa de Protección de Datos de Carácter Personal y para con lo dispuesto en el ENS.

.../...

Extraído del documento Esquema_Nacional_de_Seguridad_-_Preguntas_frecuentes

Por tanto aunque podríamos tener en cuenta la categorización de la información a nivel del ENS y de la LOPD, si nos conviene, podemos hacerlo por separado ya que: ***"...Las denominaciones BÁSICO, MEDIO y ALTO, que utilizan tanto el ENS como el Reglamento de Desarrollo de la Ley Orgánica de Protección de ... , no poseen la misma semántica. Es decir: no son intercambiables ni significan lo mismo."***

El siguiente paso evidentemente es VALORAR LOS SERVICIOS.

.../...

57. Se entiende por servicio cada actividad llevada a cabo por la Administración o, bajo un cierto control y regulación de esta, por una organización, especializada o no, y destinada a satisfacer necesidades de la colectividad.

58. El Esquema Nacional de Seguridad se limita a valorar aquellos servicios que son relevantes para el proceso administrativo, estando sometidos a la ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos. Algunos de estos servicios pueden estar identificados en algún tipo de ordenamiento general, mientras que otros serán particulares del organismo. En cualquier caso, los servicios aquí contemplados tienen identidad propia con independencia de los medios que se empleen para su prestación, asumiendo el organismo que los presta unas obligaciones con respecto a los mismos.

59. ***No se valoran servicios internos o auxiliares tales como correo electrónico, ficheros en red, servicios de directorio, de impresión, de copias de respaldo, etc.***

62. La valoración de un servicio la determina el responsable del mismo teniendo en cuenta la naturaleza del servicio y la normativa que pudiera serle de aplicación. Esta valoración requiere un conocimiento legal de la materia de que se trate.

63. Habitualmente los ***servicios establecen requisitos relevantes en términos de disponibilidad. También es habitual que los demás requisitos de seguridad sobre los servicios deriven de los de la información que se maneja.***

64. El nivel de seguridad requerido en el aspecto de ***disponibilidad se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera usar al servicio cuando lo necesita.***

65. El nivel de seguridad requerido en el aspecto de ***confidencialidad se establecerá en función de las consecuencias que tendría su revelación a alguien que no necesita conocer la información.***

66. El nivel de seguridad requerido en el aspecto de ***autenticidad se establecerá en función de las consecuencias que tendría el hecho de que el servicio fuera usado por personas indebidamente autenticadas; o sea, por personas que no son quienes se cree que son***

67. El nivel de seguridad requerido en el aspecto de ***trazabilidad se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido al servicio.***

68. Cuando un aspecto no requiere medidas de seguridad, en el apartado de valoración se indicará SIN VALORAR

…/…

Extraído de la GUÍA DE SEGURIDAD (CCN-STIC-803).

Con estas líneas, se define lo que es un servicio y además aquello que se debe valorar, y podemos eliminar de la valoración muchos de los servicios que nos preocupan, ya que *"…**No se valoran servicios internos o auxiliares tales como correo electrónico, ficheros en red, servicios de directorio, de impresión, de copias de respaldo, etc…"*** Para centrarnos sólo en lo que a nivel de categorización importa.

Ahora lo que tenemos que hacer es preparar una plantilla para los diferentes departamentos nos llenen como la de la [Tabla1], para ello preparad unas preguntas muy sencillas a la hora de determinar los niveles de impacto que tendría en las diferentes dimensiones un incidente.

Recordad el orden recomendado,
En el caso de la información sería: ***confidencialidad, integridad, autenticidad, trazabilidad y, si fuera relevante, disponibilidad.***

En el caso de los servicios: ***disponibilidad, autenticidad y trazabilidad. Los requisitos en materia de confidencialidad e integridad suelen venir impuestos por la información que maneja el servicio.***

Ejemplos:

CONFIDENCIALIDAD:
Qué se conocieran los datos de una determinada información, produciría un daño:

- Irreparable? → Alto
- Reparable? → Medio
- Fácilmente reparable? → Bajo

DISPONIBILIDAD:
Si por un incidente se para un determinado Servicio, este Servicio debe volver a prestarse:

- En menos de 4 horas. → Alto
- En un periodo de entre 4 horas y un día. → Medio
- Puede estar parado Más de 1día. → Bajo

Y así iríamos llenando la anterior tabla, al final tenemos categorizado el sistema.

Llegados a este punto sólo cabe recordar que:

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.
b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.
c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

Por último y no menos importante, se debe ***"Documentar"*** todo el proceso que ha llevado a que la categoría de un sistema sea la que hemos establecido.